P27325.A03

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant : J. L. CALVIGNAC et al. Group Art Unit: 2134

Appln No. : 09/771,472

Examiner: E. C. Tran

Filed : January 26, 2001

For : SINGLE-CYCLE HARDWARE IMPLEMENTATION OF CRYPTO FUNCTION FOR HIGH THROUGHPUT CRYPTO-PROCESSING

REQUEST FOR PRE-APPEAL BRIEF REVIEW

Commissioner for Patents
U.S. Patent and Trademark Office
Customer Window, Mail Stop AF
Randolph Building
401 Dulany Street
Alexandria, VA 22314
Sir:

This request is being filed concurrently with a Notice of Appeal and is responsive to the Final Official Action of April 21, 2005. Reconsideration and withdrawal of the single 35 U.S.C. § 102(e) rejection is respectfully requested in view of the following remarks.

A Prima Facie Case Of Unpatentability Has Not Been Set Forth And The Rejection Under 35 U.S.C. § 102(e) Is Improper

Claim 1 recites:

> a first register storing data to be encrypted or decrypted;
> a second register for receiving data which has been encrypted or decrypted; and
> combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle.

Applicants submit that COPPERSMITH is entirely silent with regard to, among other things, the recited first and second registers and/or the recited combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register in a single hardware cycle.

Examiner Arguments

In the Office Action, the Examiner asserts, that the language of COPPERSMITH

> "to provide a technique whereby the cipher used for encryption and decryption uses multiple stages, where each stage uses multiple Feistel network types that affect each word of the block"

discloses the feature

> "a first register storing data to be encrypted or decrypted, a second register for receiving data which has been encrypted or decrypted, and combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register"

as recited in claim 1.

However, the Examiner has failed to explain the equivalency between these phrases.

Applicants' Argument

Applicants submit that there is no structural or functional equivalency between the claimed language and COPPERMITH . Applicants note that the recited "combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register" language relates to the performance of computation iterations on data stored in one register and outputting data to another register. This language does not refer to performing encryption and decryption in multiple stages.

As the Examiner well knows, the term encryption broadly relates to a procedure used in cryptography to convert plaintext into ciphertext (encrypted message) in order to prevent any but the intended recipient from reading that data. Moreover, decryption broadly relates to a procedure used in cryptography to convert ciphertext (encrypted data) into plaintext. Such language is not *per se* structurally or functionally equivalent to combinational logic performing computation iterations of the crypto-function on data stored in the first register and outputting data to said second register, and the Examiner has clearly failed to demonstrate such equivalency.

Examiner Argument

The Examiner also asserts that one or more of the subprocesses of COPPERSMITH which may be embodied in a hardware chip is equivalent to the single hardware cycle of claim 1.

Applicants' Argument

The Examiner has failed to explain how the language "one or more of the subprocesses may be embodied in a hardware chip" constitutes disclosure anticipating the language "outputting data to said second register in a single hardware cycle." Applicants submit that there is no structural or functional equivalency between such language phrases. Applicants note that the recited "single hardware cycle" language relates to computation time (see page 2, lines 19-25) and not to a "hardware chip." Moreover, there is no language in COPPERSMITH indicating that the cipher functions can be completed in a single hardware cycle regardless of whether a subprocess is embodied in a hardware chip.

Applicants emphasize that COPPERSMITH uses multiple rounds, i.e., there is a setup round (Round 0) followed by subsequent rounds where the expansion box operates on the data. COPPERSMITH additionally discloses that encryption includes multiple stages, each having N rounds having N subrounds. Furthermore, operation of an expansion box requires at least one setup round and one computation round. Thus, at least two cycles of the expansion box are required for even the simplest encryption routine.

More specifically, COPPERSMITH provides a symmetric key block cipher which uses multiple stages with a modified type-3 Feistel network, and a modified unbalanced type-1 Feistel network in an expansion box forward function. Various parameters of the cipher may be varied, such as, for example, block size. The type-3 and type-1 Feistel ciphers are interleave with one another for added security.

COPPERSMITH also derives subkeys from an input key where the subkeys are used during the encryption process. The encryption process is based on a symmetric key block-oriented cipher which are well-known in the art and allows the user of the cipher to balance tradeoffs between an increased computation time versus strength of the resulting encryption. To start the encryption process of Coppersmith, subkeys are first generated using an input key. The subkeys are generated as an expanded key array. The subkeys may be generated using an iterative pseudo-random function that uses a counter and the input key as parameters. The process also includes creating a substitution box (S-box) which may be done during or before the actual encryption process. The S-box includes an array of data elements in a cipher block data word used as an index into the S-box. A value at an indexed location in the S-box is then used as an output value generated using an input key. Any pseudo-random function may be used to generate the S-box entries in a similar manner to that used for subkey generation. Additional, a key-dependent expansion box is used during each round of encryption, where the expansion box is a function implemented using a modified unbalanced type 1 Feistel network.

During the encryption phase of COPPERSMITH, encryption is performed in multiple stages where each stage includes N rounds made up of N sub-rounds where N is the number of components in the data word. Preferably, N=4 and three full stages are used for a total of 12 rounds of cipher processing. Additionally, for three full stages there are two full stages proceeded by a half stage and followed by a half stage of the cipher process, where each round consists of a modified type-3 Feistel function. Decryption is the reverse of encryption, where the same operations are run in the reverse order and the encryption operations are inverted.

Operations of the expansion box include a setup round followed by subsequent rounds of expansion box function. For example, where there are nine rounds, the first round is a setup round (Round 0) the setup round is followed by eight rounds of actual expansion box function (Rounds 1-8). In the setup round, the input is one of the data words and the data word is added to the subkey for the round creating an input value. After the setup rounds, rounds 1 through 8 are similar to each other in operation. Thus, a ciphering process will include a setup round to create an input value and is subsequently followed by one or more rounds of expansion box operation.

Accordingly, this language clearly suggests that COPPERSMITH requires multiple rounds of encryption and a hardware chip incorporating a subprocess would have to be cycled multiple times. Additionally, since the number of iterations may vary from one encryption process to the next, it would be impossible to construct a hardware circuit with circuitry which would have to cycle only once for each encryption process.

Consequently, COPPERSMITH fails to disclose combinational logic performing computation iterations of a crypto-function on data stored in a first register and outputting data to a second register in a single hardware cycle, as set forth in Claim 1. Accordingly, Claim 1 is clearly allowable over any fair reading of COPPERSMITH. Claims 2-8 are also allowable at least for the reasons discussed above with respect to independent Claim 1, from which they depend, as well as for their added features.

Reconsideration of the Final Office Action and allowance of the present application and all the claims therein are respectfully requested and now believed to be appropriate.

Respectfully submitted,
J. L. CALVIGNAC et al.

Andrew M. Calderon
Reg. No. 38,093

September 12, 2005

GREENBLUM & BERNSTEIN, P.L.C.
1950 Roland Clarke Place
Reston, VA 20191
(703) 716-1191